The Honorable Richard A. Jones

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff v. ROMAN VALEREYVICH SELEZNEV, Defendant.	NO. CR11-0070RAJ **RESPONSE TO DEFENDANT'S MOTIONS IN LIMINE** NOTED: August 3, 2016

The United States responds to defendant's Motions in Limine (Dkt. 364) as follows:

I. SCOPE OF CROSS-EXAMINATION

Consistent with the Washington Rules of Professional Conduct, this Court ruled that defense counsel may not offer evidence they know to be false or attempt to mislead the jury. Defense counsel's attempt to escape this important ruling should be rejected.

The Court's ruling was designed to "protect the integrity of the proceedings and to ensure that matters presented to the jury are grounded in good faith." Dkt. 327. Much of the proposed testimony or arguments defense counsel have outlined in their motion in limine, as well as most of defendant's proposed expert testimony, would run afoul of this goal. For example, defense expert Eric Blank's suggestion that the evidence located on

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

defendant's laptop computer was planted by the government or others is contrary to defendant's admissions and would grossly mislead the jury. While he may properly testify about computer forensic practices and whether they were properly followed in this case, any testimony that falsely suggests the government or others planted evidence is inappropriate. To the extent defense counsel's other proposed arguments or witness testimony directly contradicts specific factual statements from defendant's interview, they are not grounded in good faith.

As defendant conceded during the briefing on his earlier motion, both cases he relied on to support his motion to limit the government's use of his interview statements placed limitations on defense counsel similar to those imposed here. *United States v. Lauersen*, 2000 WL 1693538 at *8 (S.D.N.Y Nov. 13, 2000); *United States v. Burnett*, 2009 WL 2180373, at *3 (E.D. Pa. July 17, 2009). First, in *Lauersen*, after granting defendant's motion to limit the use of defendant's statements, the court went on to find that this "does not settle the matter" and stated that "the Court is duty bound to protect the integrity of the proceeding and to ensure that matters presented to the jury are grounded in good faith." *Id.* Therefore, the court concluded that "absent a good-faith basis, [defendant's] counsel may not present evidence or arguments on [defendant's] behalf that directly contradict specific factual assertions summarized in the FBI-302." *Id.* at *8.

In *Burnett*, the court entered an order identical to *Laursen* and commented in a footnote:

> The Court recognizes the opportunity for frustration this situation presents defense counsel, particularly where there can be insufficient advanced knowledge as to precisely where "the line" defense counsel must mind may be. The issue can be even more difficult for counsel in situations where, as here, one attorney is counseling the defendant at one point and another attorney handles the case for trial. *While it may be of limited solace to counsel, the Court must observe that strategic, tactical, ethical and professional challenges such as this are visited upon lawyers in a host of settings.* Skilled lawyers such as counsel in this case distinguish themselves—and well serve their clients—precisely because they see the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

> dilemma ahead of time and can try to make the best of the circumstances as presented.
>
> * * *
>
> Thus, *despite counsel's argument that the proffer agreement would "handcuff" him at trial, counsel is already "handcuffed" by the truth.* Indeed, it may well be in this instance that the defendant's waiver through the proffer agreement would not have restricted counsel any more than he was already bound by the rules of professional conduct.

Burnett, 2009 WL 2180373, at *8 n. 6 (emphases added).

Defendant's complaint that the Court's ruling "essentially" muzzles defense counsel and renders counsel ineffective is without merit for the exact reasons noted in *Burnett*. Defense counsel is not restricted by the Court's ruling so much as they are restricted by the truth. This does not mean that counsel is ineffective or unable to present an effective defense. By the explicit terms of the interview agreement, and without running afoul of the Rules of Professional Conduct, defense counsel may challenge the sufficiency of the evidence, call into question the credibility of government witnesses, question witnesses about their knowledge, qualifications, and motive to testify, and challenge inconsistencies in the evidence.

Whether defendant's proposed questions and arguments may violate the Rules of Professional Conduct will likely depend on the exact wording of the questions. If defense counsels limit their questions and arguments to challenging the adequacy of the government's proof, they will avoid running afoul of the Court's order. For example, defendant has proposed the following summary of proposed testimony and argument:

> Questions and argument contradicting the government's ability to prove that Mr. Seleznev used any or all of the nics attributed to him. For example, questions on cross-examination regarding whether agents can physically tie Mr. Seleznev to the keyboard at the time someone using the HopOne server logged on to carder.biz using the nic "bulba."

Because challenges to the sufficiency of the evidence are clearly permissible and defense counsel may properly challenge inconsistencies in the evidence, the summary above

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

would not violate the Rules of Professional Conduct. By contrast, should counsel explicitly state as part of a question or argument that Mr. Seleznev did not use the nic "bulba" or that defendant was not responsible for operating the HopOne server, this would be directly contrary to Mr. Seleznev's admissions and would therefore violate the Rules of Professional Conduct. While defense counsel may challenge the quantum of evidence as insufficient to meet the legal burden of proof, defense counsel may not argue or state explicitly that defendant did not in fact commit the acts admitted as part of his interview. If this principle is made clear, the government does not believe it necessary for the Court to rule on each of the items identified in defendant's motion.

II. GOVERNMENT'S PROPOSED SUMMARY EXHIBITS

A. Overview

Some of the most probative evidence in this case consists of dense, difficult-to-read computer information and voluminous financial records. The government has attempted to make its presentation more approachable for the jury by creating summaries that are more conveniently examined in court than the underlying data. These summaries are admissible under Federal Rule of Evidence 1006, which provides in pertinent part:

> The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation.

Fed. R. Evid. 1006. "The purpose of the rule is to allow the use of summaries when the documents are unmanageable or when the summaries would be useful to the judge and jury." *United States .v Rizk*, 660 F.3d 1125, 1130 (9th Cir. 2011) (district court properly admitted charts summarizing real estate transactions); *United States v. Aubrey*, 800 F.3d 1115, 1130 (9th Cir. 2015) (charts summarizing voluminous bank records admissible under Rule 1006).

A district court has broad discretion in determining whether to admit summaries under Rule 1006 particularly where, as the government proposes, the court also provides a cautionary instruction stating that the summary is only as good as the underlying data.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

See Government's Requested Instruction 31. *Rizk*, 660 F.3d at 1131. Summary evidence is admissible if two conditions are satisfied: the underlying materials upon which the summary is based must be (1) admissible in evidence and (2) made available to the opposing party for inspection. Fed. R. Evid. 1006; *Rizk*, 660 F.3d at 1130. The underlying materials must be admissible, but need not be admitted into evidence. *Id.* at 1130; *United States v. Meyers*, 847 F.2d 1408, 1412 (9th Cir. 1988).

Here, defendant does not contend that either of Rule 1006's conditions is unsatisfied for any of the summaries at issue. Nor could he: in each case, the underlying material is admissible and has been made available to the defense. Rather, defendant contends that the underlying records for each exhibit are not so voluminous as to justify a Rule 1006 summary. However, as described below, all of the underlying records are either voluminous or difficult to examine in court.

B. Exhibit 1.15 – Summary of Malware Installation and Mitigation

Exhibit 1.15 summarizes computer forensics evidence that Detective Dunn observed during his examinations of nine separate victim point-of-sale computer systems. *See* Attachment A – Government's Exhibit 1.15. The exhibit summarizes, by victim, relevant forensic evidence such as the date of intrusion for that victim and the location (IP address) to which defendant's malware caused the credit card data to be sent. Defendant does not dispute that the underlying evidence is admissible; nor does he contend it has not been made available to him.

Contrary to defendant's assertion, the evidence underlying Exhibit 1.15 is voluminous, unwieldy, and cannot be conveniently examined in court. It consists of computer file tables, raw malware code excerpts, internet browsing history tables, and system event logs. As the Court observed during the evidentiary hearing in this case, this computer data is extremely dense and difficult to review in its raw format – requiring extensive expert testimony to interpret and review. The government has extracted this information onto nine individual exhibits—one for each victim (*see* Attachment B –

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Government's Exhibits 1.1-1.9). Those exhibits, which are themselves admissible, are then summarized on Exhibit 1.15.

The jury will benefit from the ability reference a single table (Exhibit 1.15) that summarizes the forensic information relevant to each charged intrusion. To reach verdicts on the 40 counts in the indictment, the jury will be required to determine whether each specific intrusion and other computer event happened at certain locations on certain specific dates. Placing these locations and dates on a single summary table (which also contains references to the underlying documents) will significantly ease the jury's ability to make these determinations. Thus, these exhibits are precisely the type of "writings, recordings, or photographs which cannot conveniently be examined in court," and the use of a summary will be extremely helpful to the jury. *Rizk*, 660 F.3d 1125, 1130 (9th Cir. 2011); *see United States v. Petty*, 132 F.3d 373, 379 (7th Cir. 1997) (summaries of "unwieldy and complex" telephone records admissible under Rule 1006).

C. Exhibit 4.12 – Track2 and Bulba Domain Registration Summary

Exhibit 4.12 summarizes domain reports for five of the website domains used to facilitate the hacking and credit card trafficking scheme alleged in this case. *See* Attachment C – Government's Exhibit 4.12. A domain report is a publicly-available document listing historical registration information for a website, such as the Track2 website. As discussed in the government's Trial Brief, domain reports are admissible under Fed. R. Evid. 803(17), which allows for the admission of "directories or other compilations that are generally relied on by the public or persons in particular occupations." Dkt. 370 pp. 32-33. Again, defendant does not dispute the admissibility of the underlying data or the fact that it was produced, but merely asserts it is not voluminous.

Exhibit 4.12 summarizes five different domain reports, which together are 254 pages long. For each domain (website address), the summary sets out the email address used to register the domain, the IP address at which the domain is hosted, when the domain was created, when the registration expires. The complete reports are extremely

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

repetitive and contain a substantial amount of other data not relevant to the case. *See, e.g.,* Attachment D – Government's Exhibit 4.4 (example of one of the five reports). For example, the complete underlying domain reports include registration records for the entire history of the domain up until the date the report was run. Because many of these reports were obtained in 2016, they contain recent domain registration information post-dating the fraud that is not relevant to the case. Given the volume, complexity, and repetitiveness of these records, a summary exhibit extracting the relevant information will assist the jury and contribute to the clarity of the presentation. Allowing the jury to review a one-page summary instead of sifting through 254 pages of specialized reports is an appropriate use of Rule 1006.

D. Exhibit 4.14 – nCuX Domain Registration Summary

Exhibit 4.14 is similar to Exhibit 4.12; it simply addresses different web domains. The exhibit summarizes 48 pages of domain registration records for three domains beginning with the web address "ncux," that were used to facilitate defendant's hacking and credit card trafficking. *See* Attachment E – Government's Exhibit 4.14. Like the underlying records for Exhibit 4.12, the underlying records for exhibit 4.14 also consist of voluminous, complex and repetitive domain registration records for a time period much longer than the period relevant here. *See* Attachment F – Government's Exhibit 4.1 (example of one of the three reports). This summary is admissible for the same reasons as exhibit 4.12.

E. Exhibit 9.11 – Summary of Liberty Reserve Records

Exhibit 9.11 summarizes account records for eight separate Liberty Reserve e-currency accounts. As discussed in the government's Trial Brief, Liberty Reserve was an online e-currency system widely used by criminals as a payment system until it was closed down in 2013. Dkt. 370 at 10. Liberty Reserve records are business records admissible under Fed. R. Evid. 803(6).

Exhibit 9.11 is a summary of certain Liberty Reserve information for accounts relevant to this case (for example, accounts used to accept payment for card data sold

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

over the Track2 website). For the relevant accounts, Exhibit 9.11 sets out the account holder records, transaction histories and login IP records. *See* Attachment G – Government's Exhibit 9.11. The underlying evidence consists of thousands of pages of transaction records documenting over 68,000 transactions and thousands of login sessions.

Defendant contends that this summary should not be admitted because the underlying records are "not voluminous." As noted above, the underlying evidence consists of more than 68,000 transactions. This is clearly "voluminous" within the meaning of Rule 1006.

F. Exhibit 13.30 – Parsed Search Terms from Laptop

Exhibit 13.30 consists of computer forensic evidence that forensic examiners found in the internet history of defendant's computer. *See* Attachment H –Exhibit 13.30. The exhibit shows incidents where defendant browsed to carding–related websites, including the POS Dumps and CarderPlanet websites, and is therefore admissible to show generally his participation in the carding industry, and specifically his presence on websites he is charged with operating.

While the government's current exhibit list (perhaps confusingly) references the exhibit as a "summary," this exhibit is in fact not a summary and is not labeled as a summary on the document itself. Rather, the exhibit comprises copies of the items of forensic evidence found on defendant's computer, and therefore is admissible under Rule 1003. *See* Fed. R. Evid. 1003 (allowing for the admission of duplicates). In other words, the evidence on Exhibit 13.30 is *the evidence to be admitted*, not a summary of other underlying evidence. The exhibit therefore constitutes substantive evidence and is admissible without reference to Rule 1006. The government will be filing an amended exhibit list that does not refer to this item as a "summary."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

G. Exhibit 13.31 – Firefox Form History from Laptop

Exhibit 13.31 is similar to Exhibit 13.30. This exhibit also consists of copies of forensic evidence obtained from defendant's laptop computer. The exhibit contains a collection of terms that the user of defendant's computer had input into websites during the period leading up to his arrest. *See* Attachment I – Government's Exhibit 13.31. For example, the exhibit shows that when asked by one website for his username, defendant entered the username "2Pac." The evidence is therefore admissible to establish defendant's identity and as direct evidence of criminal activity.

As with Exhibit 13.30, Exhibit 13.31 is a copy of forensic evidence admissible under Rule 1003. Also like Exhibit 13.30, the exhibit is (inaccurately) described as a "summary" in the current exhibit list, which will be amended.

H. Exhibit 13.40 – Summary of File Dates for Items on Laptop

As the Court is aware, defendant intends to contend at trial that certain post-arrest activity on his computer may explain the existence of the incriminating files on the computer. Defendant will argue that, because the laptop was not shut down at the time of its seizure, someone must have planted the hundreds of files of incriminating evidence after his arrest. Exhibit 13.30 demonstrates that this cannot be true by establishing the critical point that none of the computer files the government will introduce was altered in any way after the arrest. Exhibit 13.40 shows this by listing, for each trial exhibit, the dates on which the file was created, last accessed and last written. *See* Attachment J – Government's Exhibit 13.40. All of the files were last written (changed) before the date of the arrest.

Exhibit 13.40 is drawn from voluminous data. The underlying evidence consists of the master file table from defendant's laptop computer, which documents these dates not just for the files relevant here (the trial exhibits), but *all* of the hundreds of thousands of files on defendant's computer. Introduction of the entire master file table would be extraordinarily confusing for the jury and would present file titles and content wholly

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

irrelevant to the case. Therefore, this summary of the file dates for the relevant exhibits is particularly appropriate for a summary exhibit.

I. Exhibit 16.14 – Summary of Travel Dates From International Passport

Defendant's passport is relevant to show his location in certain countries at certain times. However, the passport is unwieldy and difficult to examine. The passport contains more than 40 entry and exit stamps from different countries, which are scattered throughout the document. They are out of order, frequently upside down, and otherwise difficult to read without zooming in or out on the exhibit. For these reasons, the entry and exit stamps cannot be conveniently examined in court.

Government's Exhibit 16.14 is a summary of these entry and exit stamps. *See* Attachment K – Government's Exhibit 16.14. The summary exhibit summarizes the entry and exit stamps in chronological order and in a format that is easy to review and digest. Use of a summary exhibit will unquestionably assist the jury in more efficiently reviewing the information contained in the original source document.

III. TESTIMONY OF SVETLANA ZHAROVA

Defendant moves to limit the testimony of Svetlana Zharova. The government understands that Ms. Zharova has left the country. The government has been unable to effect service on Ms. Zharova, and therefore does not expect her to appear at trial. In the event the government is able to secure Ms. Zharova's attendance, the government will respond to this portion of the motion in limine accordingly.

IV. EXPERT TESTIMONY

A. "Profile" Evidence

Defendant moves to exclude "profile" testimony, citing *United States v. Gillespie*, 852 F.2d 475, 480 (9th Cir. 1988). In *Gillespie*, the Ninth Circuit held that the district court improperly admitted evidence of the personal characteristics (profile) of a typical child molester. The witness had testified that child molesters tend to have characteristics such as "early disruption of the family environment . . . a poor self-concept, and general

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

instability in their background." *Id.* *Gillespie* thus stands for the proposition that it is improper to offer evidence of the typical personal characteristics of a criminal for the purpose of showing that the defendant shares those characteristics.

The government does not intend to offer "profile" evidence of the type the Ninth Circuit rejected in *Gillespie*, that is, evidence of carders' personal characteristics. In this case, profile evidence might include evidence that carders come from certain countries, or tend to be a particular age or gender. It is easy to see why evidence of this nature might be unfairly prejudicial, and the government will not offer it.

On the other hand, the government *does* intend to offer evidence of common hacker *methodology*, which is different from their personal characteristics. For example, the government will offer testimony about different methods of intrusion, methods of stealing and marketing credit cards, and the meaning of different terms and jargon. As discussed in the government's Trial Brief, such evidence is admissible *modus operandi* testimony because it allows the jury to understand the significance of certain pieces of evidence. *United States v. Anchrum*, 590 F.3d 795, 804 (9th Cir. 2009) (law enforcement officer properly testified about *modus operandi* of gangs he had investigated); *United States v. Vallejo*, 237 F.3d 1008, 1016 (9th Cir. 2001) (expert testimony on *modus operandi* of drug dealers admissible); *United States v. Plunk*, 153 F.3d 1011, 1017 (9th Cir. 1998), *overruled on other grounds*, *United States v. Hankey*, 203 F.3d 1160, 1169 n.7 (9th Cir. 2000) (approving expert testimony on jargon and coded language of criminals). For example, the government will offer evidence defendant purchased a device known as an MSR-206, which is used to encode stolen data on a fraudulent credit card. To help the jury understand the significance of defendant purchasing an MSR-206, it is necessary to explain to the jury carders' common *methodology* of using MSR-206s to create fraudulent cards.

2. Hybrid Fact and Expert Witnesses

The government's investigating agents will testify as both fact and expert witnesses. This is necessary because investigation of cybercrime is highly specialized.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Nearly every step a Secret Service investigator takes involves the application of specialized knowledge. For an agent to explain his investigation, it is necessary for the agent to explain the specialized concepts relevant to each step of the investigation so that the testimony has meaning to the jury. The agents at times will also offer opinion testimony based on their training and experience about the meaning of the evidence.

The Ninth Circuit has held that a witness may testify as both a fact and expert witness. *United States v. Anchrum*, 590 F.3d 795, 803 (9th Cir. 2009). However, it has cautioned that there are "dangers inherent" in this practice, which stem from the fact that the witness's fact testimony may be given "unmerited credibility" when the witness has been qualified by the court an expert. *Id.* The government notes that this concern is diminished in this district, where the local practice is *not* to formally confer expert status on the witness in front of the jury. Any remaining concern should be addressed by providing the Ninth Model Instruction intended for this purpose. Ninth Circuit Model Instruction 4.14A *citing United States v. Vera*, 770 F.3d 1232, 1246 (9th Cir. 2014), *see* Government's Proposed Instruction No. 34.

The commentary to Model Instruction 4.14A states that "the court might also consider bifurcating a witness's testimony, separating a witness's percipient, or factual, testimony from the witness's expert opinions." While the government adopts this practice in many trials, it respectfully submits that this is not practical here because of the specialized nature of the investigation. As discussed above, the investigative activities of the agents (what might normally be considered the "factual" part of the investigation) are themselves so specialized that it is not possible to segregate the "factual" part of the testimony from the specialized part of the testimony. For example, to testify about a computer file an agent found on the defendant's laptop, the agent must provide specialized testimony about the type of computer file at issue. It would be hopelessly confusing to ask the witness to explain the nature of the file type during one (expert) stage of the trial and then explain his observations about the file during another (fact) stage. As the Ninth Circuit has observed, the distinction between lay and expert

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

testimony can be "a fine one," and is sometimes best "revealed through . . . cross examination." *United States v. Freeman*, 498 F.3d 893, 904 (9th Cir. 2007). This is one such case.

V. LAW ENFORCEMENT OPINION TESTIMONY

Defendant moves to prohibit opinion testimony by law enforcement officers offering the "ultimate opinion" that Roman Seleznev is guilty of the charged offenses. The government does not intend to elicit any such testimony.

VI. FDC CALLS

Defendant requests notice of any calls recorded at the FDC that it intends to offer at trial. The government does not intend to offer any such calls. With that said, all calls and their translations have been produced to the defense, and such calls would properly be admitted as non-hearsay statements, as they are statements of the defendant. Fed. R. Evid 801(d)(2). Should the government's plans change based on changed circumstances, the government will alert the defense immediately.

VII. PENDING CHARGES IN NEVADA AND GEORGIA

The defense states that the "government assured the Court and the defense that it would not offer any evidence stemming from Mr. Seleznev's pending cases" in Nevada and Georgia. This is not entirely accurate. The government stated that it would not offer evidence gathered by either of the Nevada or Georgia prosecution teams unless the government separately produced the evidence to counsel in this litigation. The purpose of this assurance was to allow counsel to limit its review, to the extent it chose to do so, to the evidence produced in this prosecution. The government will not be offering any evidence that was not directly produced to the defense in this proceeding and does not object to an order *in limine* excluding evidence from those cases not produced in this proceeding. However, defendant's request to exclude "all evidence regarding" the Nevada and Georgia charges is overly broad.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

For the most part, the pendency of the Nevada and Georgia charges are not pertinent to the government's case in chief. Nonetheless, some of the government's evidence may refer to these prosecutions. For example, Exhibit 13.36 is a webpage that defendant browsed on his laptop entitled "Cybercrime and Doing Time" that discusses the charges against defendant in Nevada. This exhibit is evidence that defendant was searching the internet for articles about himself that discussed criminal cybercrime charges. This is admissible evidence of defendant's consciousness of guilt.

VIII. EXCLUSION OF WITNESSES

Defendant requests that witnesses be excluded from the courtroom. The government does not oppose the request, but asks that the case agent, Special Agent David Mills, be exempt. A case agent is exempted from exclusion under Rule 615(b) and (c), which permit the attendance of a party's "representative" or a person whose presence is "essential" to presenting the party's claim. *See* Rule 615 Adv. Comm. Note (noting that many courts allow the "government to have an investigative agent at counsel table"); *United States v. Thomas*, 835 F.2d 219, 222-23 (9th Cir. 1987) (noting that under Ninth Circuit law, case agent should be permitted to sit in trial "as an officer for the government"). The government may also seek an exemption to allow its rebuttal experts to hear the testimony of any expert tendered by the defense, but will raise that issue, if necessary, when it arises.

IX. WITNESSES DISCUSSING THE CASE

Defendant requests that witnesses be forbidden from speaking to one another about their testimony. The government has no objection to this request and will so inform its witnesses. In kind, the government requests the Court to instruct the defense to advise its potential witnesses similarly.

X. ADVANCE NOTICE OF WITNESS ORDER

Defendant requests 48 hours' advance notice of witness order. The government does not object to providing advance notice of witness order, but it may not always be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

possible to accurately predict the order of witnesses 48 hours ahead of time. At the end of each trial day, the government will inform the defense of its expected order for the following day.

DATE: July 29, 2016.

ANNETTE L. HAYES
Acting United States Attorney

/s/ Norman M. Barbosa
NORMAN M. BARBOSA
Assistant United States Attorney
Western District of Washington

/s/ Seth Wilkinson
SETH WILKINSON
Assistant United States Attorney

LESLIE R. CALDWELL
Assistant Attorney General

/s/ Harold Chun
HAROLD CHUN
Trial Attorney
Computer Crime and Intellectual Property Section

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF SERVICE

I hereby certify that on July 29th, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the attorney of record for Defendant.

s/ Jennifer J. Witt

JENNIFER J. WITT
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: 206-553-2520
Fax: 206-553-2502
E-mail: Jennifer.Witt@usdoj.gov